DOCKET NO.: 51876P585

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

SOO-HYUNG LEE, ET AL.

Application No.:

Filed:

For: **Method for Detecting Abnormal Traffic at Network Level Using Statistical Analysis**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Republic of Korea	2003-81833	18 November 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 12/31/03

William Thomas Babbitt, Reg. No. 39,591

12400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0081833
Application Number

출 원 년 월 일 : 2003년 11월 18일
Date of Application NOV 18, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Inst

2003 년 12 월 04 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2003.11.18

【발명의 명칭】 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법

【발명의 영문명칭】 Method for detecting abnormal traffic in network level using statistical analysis

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【명칭】 특허법인 신성

【대리인코드】 9-2000-100004-8

【지정된변리사】 변리사 정지원, 변리사 원석희, 변리사 박해천

【포괄위임등록번호】 2000-051975-8

【발명자】

【성명의 국문표기】 이수형

【성명의 영문표기】 LEE,Soo Hyung

【주민등록번호】 690429-1670218

【우편번호】 305-345

【주소】 대전광역시 유성구 신성동 하나아파트 107-1006

【국적】 KR

【발명자】

【성명의 국문표기】 장범환

【성명의 영문표기】 CHANG,Beom Hwan

【주민등록번호】 711213-1347912

【우편번호】 305-503

【주소】 대전광역시 유성구 송강동 송강마을아파트 203-1106

【국적】 KR

【발명자】

【성명의 국문표기】 김진오

【성명의 영문표기】 KIM,Jin Oh

【주민등록번호】 670104-1226221
【우편번호】 305-729
【주소】 대전광역시 유성구 전민동 청구나래아파트 109-1306
【국적】 KR

【발명자】
【성명의 국문표기】 나중찬
【성명의 영문표기】 NA,Jung Chan
【주민등록번호】 620725-1408216
【우편번호】 305-333
【주소】 대전광역시 유성구 어은동 한빛아파트 121-206
【국적】 KR

【발명자】
【성명의 국문표기】 손승원
【성명의 영문표기】 SOHN,Sung Won
【주민등록번호】 571225-1674514
【우편번호】 305-390
【주소】 대전광역시 유성구 전민동 엑스포아파트 208-902
【국적】 KR

【발명자】
【성명의 국문표기】 박치항
【성명의 영문표기】 PARK,Chee Hang
【주민등록번호】 470112-1069516
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 131-1002
【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
특허법인 신성 (인)

【수수료】

【기본출원료】	17	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	4	항	237,000 원

【합계】 266,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 133,000 원
【기술이전】
【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 네트워크상의 각 네트워크 장비로부터 수집한 트래픽 데이터를 네트워크 수준의 전체 트래픽 데이터로 통합하여 이상 트래픽 감지에 이용되는 특성 트래픽 데이터를 추출한 후 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 단시간내에 이상 트래픽을 감지하기 위한, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록메체를 제공하는데 그 목적이 있음.

3. 발명의 해결방법의 요지

본 발명은, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 있어서, 소정의 시간 간격으로 네트워크의 각 네트워크 장비로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하는 제 1 단계; 상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출하는 제 2 단계; 상기 추출한 특성 트래픽 데이터를 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽 여부를 판단하는 제 3 단계; 및 상기 판단결과, 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터를 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고, 이상 트래픽이면 현

재 발생한 트래픽의 심각도를 분석하고 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링하는 제 4 단계를 포함한다.

4. 발명의 중요한 용도

본 발명은 네트워크 보안 시스템 등에 이용됨.

【대표도】

도 3

【색인어】

이상 트래픽 감지, 특성 트래픽 데이터, 특성 트래픽 데이터 프로파일, 네트워크 수준, 통계적 분석

【명세서】

【발명의 명칭】

통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법{Method for detecting abnormal traffic in network level using statistical analysis}

【도면의 간단한 설명】

도 1 은 종래의 네트워크상에서 이상 트래픽 감지 방법에 대한 일실시예 설명도.

도 2 는 본 발명에 따른 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 대한 일실시예 설명도.

도 3 은 본 발명에 따른 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 대한 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호의 설명

210 : 네트워크 장비 211 : 네트워크 보안 시스템(NSS)

212 : 로컬 도메인

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로, 더욱 상세하게는 네트워크의 성능을 저하시키는 사이버 공격 또는 네트워크 구성 및 운용상의 결함 등으로 인하여 발생하는 이상 트래픽을 단시간내에 감지하기 위한, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

<8> 일반적으로, 네트워크상에서 발생한 이상 트래픽을 감지하는 방법은 현재 수집한 트래픽량과 통계적으로 생성된 정상 상태를 나타내는 트래픽량의 비교값 또는 비교 그래프 등을 모니터링하여 관리자가 상기 모니터링된 비교값과 비교 그래프를 경험적으로 분석함으로써, 현재 네트워크상에 발생한 트래픽이 이상 트래픽인지의 여부를 판단하게 된다.

<9> 여기서, 이상 트래픽이란 네트워크의 성능을 저하시킬 수 있는 데이터들이 비정상적으로 증가하여 네트워크의 흐름을 방해하는 상태를 의미하며, 그 원인으로는 사이버 공격에 의한 직간접적인 영향 또는 네크워크 구성 및 운용상의 결함 또는 클라이언트들의 과다 접속 등으로 발생한다.

<10> 도 1 은 종래의 네트워크상에서 이상 트래픽 감지 방법에 대한 일실시예 설명도이다.

<11> 도 1 에 도시된 바와 같이, 하나의 네트워크(ISP 1: Internet Service Provider 1)는 다수의 로컬 도메인(112), 타 네트워크(ISP 2), 상기 네트워크(ISP 1)와 로컬 도메인 또는 상기

네트워크(ISP 1)와 타 네트워크(ISP 2)를 연결하는 다수의 네트워크 장비(일예로 라우터)(110) 및 상기 네트워크(ISP 1)를 관리하기 위한 네트워크 관리 서버(NMS: Network Management Server)(111)를 포함한다.

<12> 여기서, 도 1 을 참조하여 종래의 네트워크상에서 이상 트래픽 감지 방법에 대해 살펴보면, 먼저 상기 네트워크 장비(110)에는 관리 에이전트가 설치되어 있어 노드 또는 특정 도메인 또는 링크상에서 처리되는 트래픽 데이터(정보)를 수집하는 기능을 한다.

<13> 이후, 네트워크 관리 서버(111)는 네트워크상의 각 네트워크 장비(110)로부터 트래픽 데이터를 수집하여, 관리 콘솔을 통하여 해당 트래픽 정보를 관리자에게 보고하게 된다.

<14> 이후, 과다 트래픽 발생 여부는 관리자가 네트워크 관리 서버가 보고하는 트래픽 데이터를 바탕으로 하여 과거 경험에 의해 직관적으로 판단하게 된다.

<15> 이러한 종래의 네트워크상에서 이상 트래픽 감지 방법은, 수집하는 트래픽량이 대부분 특정 로컬 도메인(특정 링크 또는 특정 노드)에서 발생하는 단순 트래픽량만을 대상으로 하는 경우가 대부분이고, 관리자가 현재 발생한 트래픽이 해당 네트워크의 성능을 저하시킬 수 있는 트래픽(이상 트래픽)인지, 아닌지의 여부를 판단하기 때문에 단시간내에 정확한 판단을 할 수 없다는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<16> 본 발명은 상기 문제점을 해결하기 위하여 제안된 것으로, 네트워크상의 각 네트워크 장비로부터 수집한 트래픽 데이터를 네트워크 수준의 전체 트래픽 데이터로 통합하여 이상 트래픽 감지에 이용되는 특성 트래픽 데이터를 추출한 후 정상 상태의 통계적 모델인 특성 트래픽

데이터 프로파일과 비교하여 단시간내에 이상 트래픽을 감지하는, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록메체를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<17> 상기 목적을 달성하기 위한 본 발명의 방법은, 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 있어서, 소정의 시간 간격으로 네트워크의 각 네트워크 장비로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하는 제 1 단계; 상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출하는 제 2 단계; 상기 추출한 트래픽 특성 데이터를 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽 여부를 판단하는 제 3 단계; 및 상기 판단결과, 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터를 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고, 이상 트래픽이면 현재 발생한 트래픽의 심각도를 분석하고 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링하는 제 4 단계를 포함하는 것을 특징으로 한다.

<18> 한편, 본 발명은, 프로세서를 구비한 이상 트래픽 감지 시스템에, 소정의 시간 간격으로 네트워크의 각 네트워크 장비로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하는 제 1 기능; 상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출하는 제 2 기능; 상기 추출한 트래픽 특성 데이터를 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽 여부를 판단하는 제 3 기능; 및 상기 판단결과, 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터를 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고, 이상 트래픽이면 현재 발생한 트래픽의 심각도를 분석

하고 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링하는 제 4 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<19> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<20> 도 2 는 본 발명에 따른 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 대한 일실시예 설명도이다.

<21> 도 2 에 도시된 바와 같이, 이상 트래픽 감지 모듈을 장착한 네트워크 보안 시스템(NSS: Network Security System)(211)은 네트워크 장비(일예로 라우터)(210)를 통해 다수의 로컬 도메인(212) 또는 타 네크워크(ISP 2)와 연결되어 있다. 이 때, 상기 네트워크 장비(210)는 네트워크상의 로컬 도메인(링크) 또는 타 네트워크(ISP2)로부터 트래픽 데이터(정보)를 수집하는 기능을 수행한다.

<22> 여기서, 도 2 를 참조하여 본 발명에 따른 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 대해 살펴보면, 본 발명은 네트워크 보안 시스템(211) 등에 적용되어 네트워크상의 각 네트워크 장비(210)로부터 주기적으로 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하고 상기 통합된 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출한 후, 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽을 감지한다.

<23> 이 때, 상기 네트워크 수준의 전체 트래픽 데이터에서 특성 트래픽 데이터를 추출하는 기준은, 일예로 응용 서비스의 종류에 따라 각기 다르게 할당되는 응용포트에 따라 추출하거나

, 동일한 크기를 가진 패킷분포에 따라 추출하거나, 특정 목적지(destination)로 가는 트래픽의 원천지(source) 주소가 급격히 증가하는 패턴을 바탕으로 한 원천지-목적지 페어(source-destination pair)수 등에 따라 추출할 수 있다.

<24> 또한, 트래픽 데이터 수집은 기존의 네트워크 관리 시스템에서와 같이 일반적으로 네트워크 노드상에 설치되는, 네트워크 관리 에이전트를 장착한 네트워크 장비(일예로 라우터)의 트래픽 수집 기능을 이용하여 기존 네트워크상에서 이용되는 네트워크 장비의 교체없이 트래픽 데이터를 수집한다.

<25> 또한, 네트워크 보안 시스템은 타 네트워크 보안 기능을 수행할 수 있으며, 이상 트래픽 감지 측면에서 수행할 기능은 통계 분석 모듈을 탑재함으로써, 일정 주기로 트래픽 데이터를 수집하고 정상 상태의 통계적 트래픽 특성과 비교 분석하여 이상 트래픽을 감지하는 기능을 수행한다. 이 때, 현재 수집된 트래픽이 이상 트래픽으로 판단되면 현재 발생한 트래픽이 얼마나 심각한지를 분석하고, 그 결과를 데이터로 생성한다.

<26> 이후, 상기 데이터는 추후 네트워크 보안 시스템의 타 보안 기능과 결합하여 관리자에게 보고용으로 사용될 수도 있고, 네트워크 보안 시스템의 보안 대응 기능과 결합하여 네트워크상에서 자동적인 대응이 이루어지도록 할 수도 있다.

<27> 도 3 은 본 발명에 따른 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 대한 일실시예 흐름도이다.

<28> 먼저, 사용자로부터 이상 트래픽이 발생했을 경우의 심각도 유의 수준, 트래픽 분석 주기, 분석 결과의 처리 방식 등의 실행 환경을 설정받는다. 물론 데이터 베이스에는 최근까지 통계적으로 생성한 특성 트래픽 데이터 프로파일이 저장되어 있다.

<29> 이후, 소정의 시간 간격으로 각 네트워크의 장비(210)로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합한다(301, 302).

<30> 이후, 상기 네트워크 수준의 전체 트래픽 데이터로부터 상기 언급한 소정의 추출 기준에 따라 특성 트래픽 데이터를 추출한다(303).

<31> 이후, 상기 추출한 트래픽 특성 데이터를 정상 상태의 트래픽을 모델링하여 파라미터화한 특성 트래픽 데이터 프로파일과 비교하여 현재 트래픽이 이상 트래픽인지 정상 트래픽인지를 판단한다(304, 305).

<32> 상기 판단결과(305), 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터을 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고 일정시간 대기한 후 상기 "301" 과정으로 진행하여 이후의 과정을 수행한다(306). 이러한 과정은 다양한 정상 상태 트래픽을 통계적으로 데이터베이스화하는 과정으로 보다 정확한 이상 트래픽 감지를 위해 꼭 필요한 과정이라 할 수 있다.

<33> 상기 판단결과(305), 이상 트래픽이면 상기 기 설정된 심각도 유의 수준에 따라 현재 발생한 트래픽의 심각도를 분석하고(307), 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링한다(308). 이 때, 상기 분석결과와 이상 트래픽에 대한 정보를 이상 트래픽 처리 시스템 등으로 전달하여 효율적인 이상 트래픽 처리에 이용되도록 할 수도 있다.

<34> 이처럼 본 발명은 주기적으로 네트워크상에 발생하는 트래픽을 검사하여 이상 트래픽을 감지한다.

<35> 또한, 본 발명은, 네트워크 장비(210)로부터 직접 특성 트래픽 데이터를 수집하여 이상 트래픽을 감지할 수도 있다. 하지만, 이러한 방법은 네트워크 장비(210)의 부하를 가중시키는 역효과가 있을 수 있다.

<36> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

<37> 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

【발명의 효과】

<38> 상기와 같은 본 발명은, 네트워크상에서 발생하는 트래픽 전체에 대해 특성 트래픽 데이터를 추출하여 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교함으로써, 효율적으로 빠른 시간내에 이상 트래픽을 감지할 수 있도록 하는 효과가 있다.

<39> 또한, 본 발명은, 다양한 정상 상태 트래픽을 통계적으로 데이터베이스화하는 과정을 통해 관리자의 개입없이 자동으로 보다 다양한 형태의 이상 트래픽을 감지할 수 있도록 하는 효과가 있다.

<40> 또한, 본 발명은, 이상 트래픽 처리 시스템에 적용되어 네트워크의 기능이 마비되기 전에 이상 트래픽을 처리할 수 있도록 하는 효과가 있다.

【특허청구범위】

【청구항 1】

통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법에 있어서,

소정의 시간 간격으로 네트워크의 각 네트워크 장비로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하는 제 1 단계;

상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출하는 제 2 단계;

상기 추출한 특성 트래픽 데이터를 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽 여부를 판단하는 제 3 단계; 및

상기 판단결과, 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터를 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고, 이상 트래픽이면 현재 발생한 트래픽의 심각도를 분석하고 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링하는 제 4 단계

를 포함하는 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법.

【청구항 2】

제 1 항에 있어서,

상기 특성 트래픽 데이터는,

서비스의 종류에 따라 각기 다르게 할당되는 응용포트에 따라 추출한 특성 트래픽 데이터 또는 동일한 크기를 가진 패킷분포에 따라 추출한 특성 트래픽 데이터 또는 특정 목적지(destination)로 가는 트래픽의 원천지(source) 주소가 급격히 증가하는 패턴을 바탕으로 한

원천지-목적지 페어(source-destination pair)수에 따라 추출한 특성 트래픽 데이터인 것을 특징으로 하는 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 심각도 분석결과와 이상 트래픽에 대한 정보를 이상 트래픽 처리 시스템으로 전달하여 효율적인 이상 트래픽 처리에 이용되도록 하는 제 5 단계

를 더 포함하는 통계적 분석을 이용한 네트워크 수준에서의 이상 트래픽 감지 방법.

【청구항 4】

프로세서를 구비한 이상 트래픽 감지 시스템에,

소정의 시간 간격으로 네트워크의 각 네트워크 장비로부터 트래픽 데이터를 수집하여 네트워크 수준의 전체 트래픽 데이터로 통합하는 제 1 기능;

상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터를 추출하는 제 2 기능;

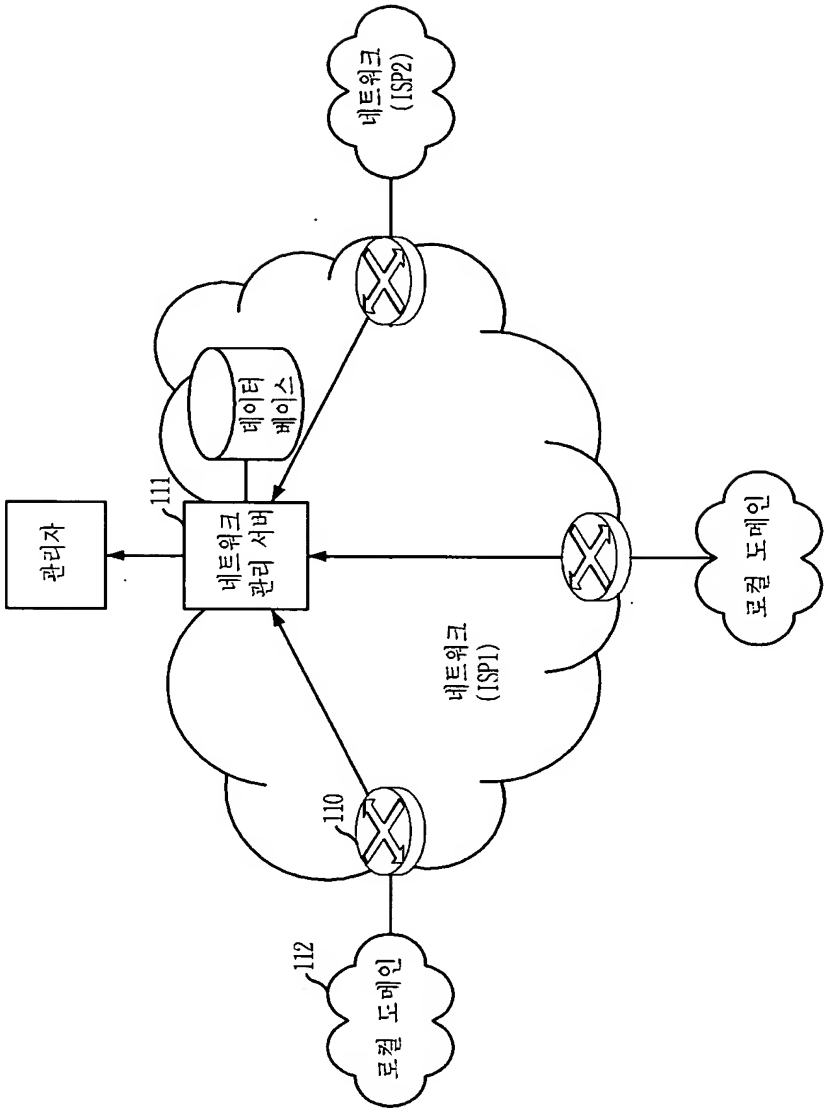
상기 추출한 트래픽 특성 데이터를 정상 상태의 통계적 모델인 특성 트래픽 데이터 프로파일과 비교하여 이상 트래픽 여부를 판단하는 제 3 기능; 및

상기 판단결과, 이상 트래픽이 아니면 상기 추출한 트래픽 특성 데이터를 이용하여 상기 특성 트래픽 데이터 프로파일을 갱신(업데이트)하고, 이상 트래픽이면 현재 발생한 트래픽의 심각도를 분석하고 상기 분석결과와 이상 트래픽에 대한 정보를 모니터링하는 제 4 기능

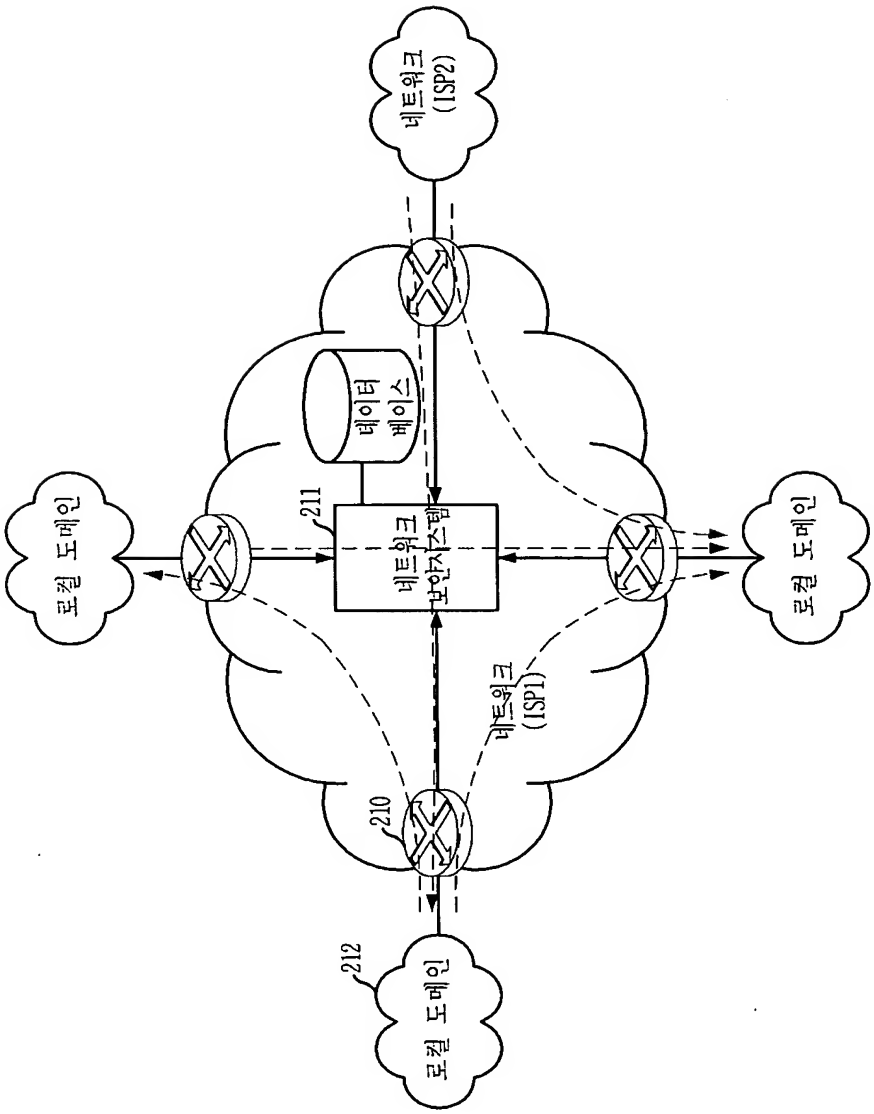
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

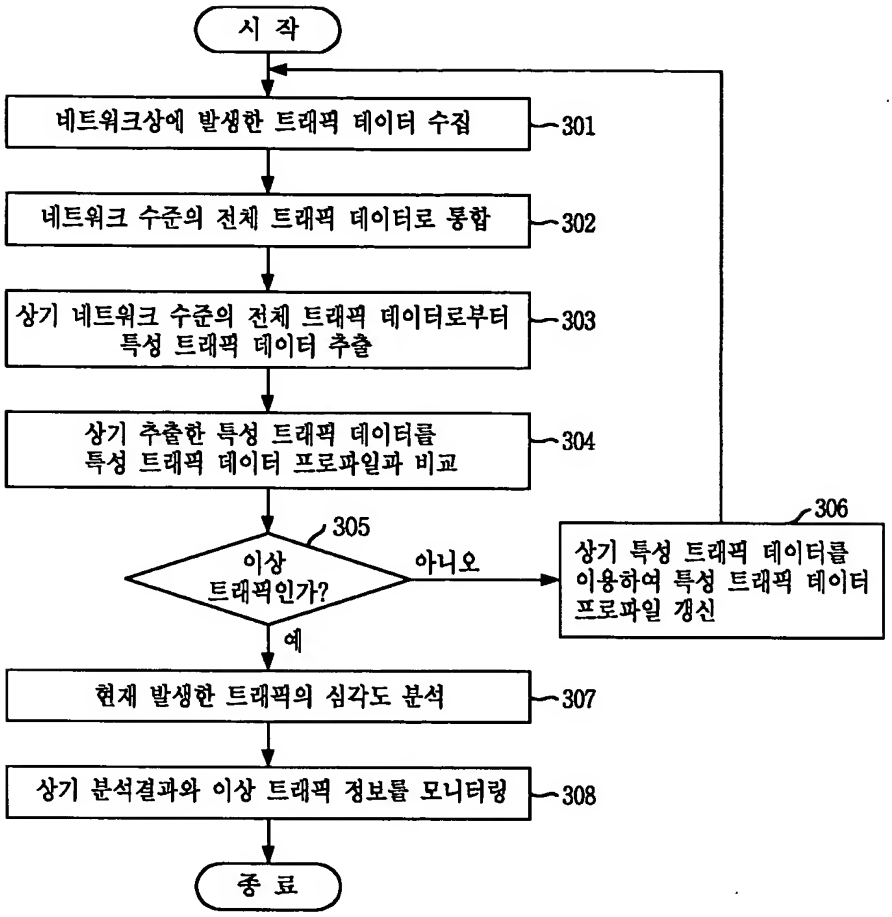
【도 1】


네트워크
(ISP2)
데이터
베이스
111
관리자
네트워크
관리 서버
로컬 도메인
네트워크
(ISP1)
110
112
로컬 도메인

【도 2】


네트워크
(ISP2)
데이터
베이스
211
네트워크
보안지원템
로컬 도메인
로컬 도메인
네트워크
(ISP1)
210
212
로컬 도메인

【도 3】


시 작
네트워크상에 발생한 트래픽 데이터 수집
301
네트워크 수준의 전체 트래픽 데이터로 통합
302
상기 네트워크 수준의 전체 트래픽 데이터로부터 특성 트래픽 데이터 추출
303
상기 추출한 특성 트래픽 데이터를 특성 트래픽 데이터 프로파일과 비교
304
305
이상 트래픽인가?
아니오
306
상기 특성 트래픽 데이터를 이용하여 특성 트래픽 데이터 프로파일 갱신
예
현재 발생한 트래픽의 심각도 분석
307
상기 분석결과와 이상 트래픽 정보를 모니터링
308
종 료